Smart Regulation and the General Data Protection Regulation

Dr Asma Vranaki*

* *Asma is an Associate Fellow at the University of Oxford where she investigates the regulation of computer-mediated communication technologies (e.g. cloud computing, social media). She is a non-practising barrister who specialises in the data protection and privacy law issues raised by the Digital Age.*

Data protection and privacy practitioners are waiting anxiously for the official adoption of the General Data Protection Regulation ("GDPR"). The latest indication from the European Commission is that the GDPR will officially be adopted in June/July 2016 and in force as from June/July 2018.

Since political agreement has been reached on the GDPR in December 2015, we have a fairly good idea of some of the main aspects of the official legislation, such as the statutory recognition of an "accountability" principle, a risk-based approach to data protection (e.g. data protection/privacy impact assessments, privacy by design, breach notification), and enhanced individual rights (e.g. new right of data portability and right to be forgotten).

Once the GDPR is in force, the litmus test for success will be the consistent implementation, interpretation and enforcement of the Regulation. Many commentators have already warned that the GDPR's promise of harmonization may be more fiction than fact due to the vague and ambiguous provisions of the GDPR (e.g. legitimate interests provision) as well as the so-called "open clauses". "Open clauses" refer to the GDPR provisions whose implementation are left to the member-states.

But looking beyond the immediate parapet of the rules, the GDPR is also heralding a move to smart regulation. One aspect of smart regulation is that it involves interactions between diverse stakeholders, such as law-makers, EU DPAs, European Data Protection Board, European Commission, data controllers, data processors, and quasi-regulators (e.g. third-party certification bodies). Some of these stakeholders, such as EU DPAs and the companies they regulate, used to interact with one another in the pre-GDPR era. However, a move towards smart regulation can often impact on these existing relationships.

In this article, I explore what smart regulation may mean for the relationships between EU DPAs and the companies they regulate. I draw on some of the findings of my recent empirical research project, where I have analysed how some EU DPAs are starting to embrace smart regulation during their investigations of multinational cloud providers, to suggest **four** potential key aspects of a smart regulatory relationship between EU DPAs and their regulatees. These **four** points are mere starting points when reflecting on what smart regulation may look like for the relationships between EU DPAs and the companies they oversee. As noted below, much more work needs to be done to flesh out how such relationships will be developed in practice.

Active Engagement between EU DPAs and Companies

Companies and EU DPAs will benefit from active, regular, and informal engagement with each other from the very beginning and in any event before a data breach is detected or reported. Opening the dialogue between the regulator and regulatees from an early stage has three key advantages. Firstly, it will enable both parties to build a productive rapport which will be crucial

in many cases where there will be a long-term relationship between the regulator and the company. This will, in all likelihood, be the case for multinational companies with a strong European presence and the EU DPAs which will be their lead regulator for their European operations.

Secondly, this type of interaction will make it possible for EU DPAs to gain an in-depth knowledge of the processing operations and policies of the companies which fall within their jurisdiction, long before any data breach has been reported.

Finally, this will provide companies with the opportunity to explain to the regulators their offerings, business drivers, and processing operations. Such engagement means that the regulator will have a detailed understanding of the organization which can often be useful during enforcement. Organisations can also discuss with EU DPAs the data protection and privacy issues which are potentially raised by their future products or services and tackle such issues head on at the ideation or preliminary design stage rather than after these products or services have been launched. This approach can often not only be cost-effective but also enable companies, especially multinationals, to reduce or avoid negative media coverage which plays a pivotal role in determining the reputation of such organisations.

This level of engagement between EU DPAs and companies will be problematic if EU DPAs do not develop effective and consistent strategies which will enable them to prioritise tasks in an informed and systematic way. This will be even more crucial for EU DPAs which have limited resources. Unfortunately, the GDPR is silent on how EU DPAs can assess the priority of their activities. Consequently, one of the task ahead before the GDRP is in force will be to formulate consistent guidelines which EU DPAs can use to evaluate which regulatory activity takes precedence over others.

Compliance Attitudes of Companies

EU DPAs will need to recognize that companies will have different, and often complex attitudes to compliance. Some organisations may be largely co-operative whilst others may often be recalcitrant. Additionally, the compliance attitudes of companies are likely to change over time for various reasons including media coverage, reputation, change in management and so on. At times, an otherwise co-operative company can start to object to some of the data protection recommendations which an EU DPA may make. Consequently, EU DPAs need to learn how to deal with and manage the intricate and rapidly evolving compliance attitudes of the organisations they oversee.

Additionally, EU DPAs may often benefit from identifying the reasons why companies may wish to comply with the law. EU DPAs can then often use these reasons as bargaining chips during their interactions with these organisations in order to secure the desired data protection outcome. In many cases, compliance can often be driven by many (rather than one), often interconnected reasons, such as avoiding reputational damage, generating the trust of customers in the company, avoiding citable binding court decisions, and moral reasons.

Dynamic Regulatory Styles

EU DPAs may benefit from developing dynamic regulatory styles so that they can respond effectively to the diverse and often shifting compliance attitudes of their regulatees. In particular, in some cases it may be appropriate for EU DPAs to adopt regulatory styles which gradually

escalate from soft strategies (e.g. persuasion, discussion) to harder strategies where the regulatee objects to base line compliance (e.g. threat to initiate enforcement action) to soft strategies again once the organization co-operates.

My recent study highlighted that regulatory styles which can seamlessly move from one end of the spectrum (soft) to the other (hard) and back are often the most effective ones. Additionally, my research also showed that EU DPAs which adopted a "smarter" approach to regulation by adopting not only dynamic regulatory styles but also recognising the business drivers of companies, attempting to find mutually convenient solutions, and not relying heavily on formalistic tools often achieved better outcomes in the longer term.

This shift in the regulatory styles of EU DPAs will be one of the key challenges ahead when tackling smart regulation. Some EU DPAs may be bound by procedural rules which may prevent them from smoothly moving from soft to hard to soft regulatory styles. Other EU DPAs may need to learn how to regulate in this manner whilst being effective. Thus, we need to bear these points in mind when thinking about how to develop smart regulation when the GDPR is in force.

Regulatory relationship management

Smart regulation also means that companies need to rethink how they approach and manage their relationships with the EU DPAs. In the *pre-GDPR* era, the regulatory relationship often started on an *ex-post* basis, for example, when a data breach was detected or when an individual filed a complaint against the company. In many cases, the regulatory relationship would often start on negative note with many companies being on the defensive from the start.

In the *GDPR era*, the relationships between many companies (let's say multinationals) and their regulators, especially their lead EU DPAs, may often be from cradle to grave. Such relationships may often start on an *ex-ante* basis, for example, when a multinational opens a local branch in the territory of the EU DPA.

In order to develop healthy and productive regulatory relationships, many organisations will have to change how conceive and manage these relationships. We may need to look at how regulatory relationships in other industries are successfully built in order to learn how companies can build effective and long-term relationships with EU DPAs.

For example, showing the regulators that you want to co-operate (and mean it!), knowing how to negotiate compliance effectively so as to promote innovation whilst complying with the law, keeping the promises made to the regulators may be fruitful ways in which companies can start creating a positive dialogue with their regulators. We also need to consider how SMEs and other companies with limited budget can cultivate this type of regulatory relationship despite their limited resources.

For more see, Vranaki, Asma A.I., "Cloud Investigations by European Data Protection Authorities: An Empirical Account," in Rothchild John A (ed), *Research Handbook on Electronic Commerce Law* (Edward Elgar, Forthcoming); Queen Mary School of Law Legal Studies Research Paper No. 195/2015 < http://ssrn.com/abstract=2602216>. The author conducted this research whilst working on the EC-funded "Accountability for Cloud" research project.